

Office of Inspector General



June 18, 2001
Audit Report No. 01-017

Receivership Liability System Security and Data Validation



DATE: June 18, 2001

TO: Donald C. Demitros, Director
Division of Information Resources Management and
Chief Information Officer

Mitchell L. Glassman, Director
Division of Resolutions and Receiverships



FROM: Russell A. Rau
Assistant Inspector General for Audits

SUBJECT: *Audit of Receivership Liability System Security and Data Validation*
(Audit Report No. 01-017)

This report presents the results of an audit of the Federal Deposit Insurance Corporation's (FDIC) security and controls over the initial loading of data into its Receivership Liability System (RLS). This is the second audit that the Office of Inspector General (OIG) has performed on RLS. On December 28, 2000, the OIG issued a report entitled *Receivership Liability System Staffing and Training* (Audit Report No. 00-051) in which we reported that the Division of Resolutions and Receiverships (DRR) and the Division of Information Resources Management (DIRM) had adequately planned for reduced RLS-related staffing levels resulting from corporate downsizing but needed to improve training.

BACKGROUND

One of the FDIC's critical missions is to resolve insolvent financial institutions. It is the responsibility of DRR's Dallas Field Operations Branch (DFOB) to identify and process claims from depositors and general creditors of failed financial institutions. DFOB claims personnel attend bank closings, determine deposit insurance coverage, identify all general creditors and those depositors with balances in excess of deposit limitations, perform payouts, track claims, and perform customer service functions.

To assist DRR with its claims responsibilities, DRR and DIRM developed RLS at a cost of almost \$9.5 million as of February 2001. RLS will eventually replace three separate "legacy" systems that preceded RLS. These legacy systems are the (1) Claims Tracking System (CTS), (2) Automated Grouping System/Automated Payout System (AGS/APS), and (3) Unclaimed Deposit Reporting System (UDRS). At the time of our audit, DIRM and DRR were concentrating their efforts on converting data from the CTS. Conversion of data from the

AGS/APS and UDRS is to follow at an unspecified date. From July 1999 (when RLS was first used at the closing of a financial institution) through March 2001, DFOB claims personnel used RLS at 14 institution closings with a total deposit base of over \$1.6 billion.

RLS is a tracking system for individual claims that also provides summary data. RLS uses a sophisticated Microsoft Structured Query Language (SQL) server relational database. The database consists of more than 40 tables of data that are updated, following data entry, in a complex sequence of steps that results in multiple tables being updated for a single transaction. The system is designed with initial data edits that permit properly formatted and complete records to be entered into the system. The system includes multiple layers of user access authorizations and administrator restrictions to deter unauthorized access. DIRM and DRR have also implemented audit tables that capture activity in the daily production environment.

For purposes of this report it is important to note that RLS functions in three separate operational environments. As described in the December 29, 1999 draft of the FDIC's *RLS Operations Manual*, these three operational environments are linked to activity before, during, and after an institution's closing, as discussed below:

- **Pre-Closing.** The RLS pre-closing environment supports the "estimations" server. The database on the estimations server contains information from either a distressed financial institution or one that may potentially fail. Claims evaluates the institution's deposits to determine the number of deposits in excess of insured amounts for inclusion in DRR's institution resolution work. This database executes on an SQL server not connected to the FDIC network. The estimations server is located in Dallas, Texas, and is not available to users nationwide from their desktops. The database must be accessed directly from the estimations server consoles or from personal computers connected to the server.
- **Closing.** RLS portable local area networks (LAN) used during an institution closing are operated at the institution closing site. The portable LAN supports RLS processing for the specific institution being closed. After the RLS portion of the closing is complete, DIRM transmits the closing data from the RLS portable LAN to the national database located in the FDIC's main computer facility in the Washington, D.C., area (Virginia Square).
- **Post-Closing.** The national database is used to complete the processing of failed institutions' liabilities. It is run on an SQL server on the FDIC network and is accessed on claims agents' individual workstations. The national database will contain data from all institution closings once the process of data conversion from the legacy systems is complete.

Each of these environments represents a distinct challenge for the FDIC. Physical security considerations may differ as well as the numbers and types of DRR and DIRM personnel needing access to the particular RLS environment.

DIRM and DRR are jointly responsible for the successful operation of RLS. DIRM personnel provide technical support for RLS to operate on an ongoing basis as well as at bank closings. DIRM supports RLS by administering the various databases used by DRR personnel, shipping and operating the FDIC's computer equipment at bank closings, downloading institution data

into RLS, supporting data processing, transmitting data, and shipping the computer equipment back to the FDIC. However, it is the responsibility of DRR personnel to enter, edit, approve, process, and analyze the data in RLS.

In total, seven DRR and DIRM groups are responsible for the operations of RLS. These groups include: DRR security staff, DRR claims personnel, DRR data stewards, DIRM system developers, DIRM Microsoft SQL server system administrators, DIRM database administrators, and DIRM Dallas personnel. With so many groups involved in system operations, it is critical to have clear assignments of functional responsibilities. Without clear assignments of functional responsibilities, necessary security measures may not be effectively implemented and followed. The FDIC assigned RLS the highest data sensitivity ranking for a DRR system, as identified in the September 2000 *Sensitivity Assessment Questionnaire*. This ranking designates that the data is of an extremely sensitive nature and should be adequately protected from accidental or intentional disclosure, modification, or alteration. Specifically, RLS contains private and sensitive information including depositor name, address, social security number, and account balance information that could be used in identity theft—a growing concern for law enforcement agencies. Further, the estimations database contains information on potentially troubled banks—information that needs to be carefully safeguarded.

Successful deployment of RLS helps DRR accomplish portions of its 2001 Strategic Plan. For example, one of the performance goal targets is: “Insured deposits are transferred to assuming bank or deposit payouts are begun within 1 business day if the failure occurs on Friday, or 2 business days if the failure occurs on any other day.” We believe RLS must function as flawlessly as possible to achieve this goal. Also, we believe information and recommendations in this report will help DRR achieve another 2001 Strategic Plan objective, “Review and update insured bank resolution/closing policies and procedures to improve processes . . .”

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of our audit were to (1) determine whether the security environment over RLS is adequate and (2) identify vulnerabilities that could hamper the accurate and complete initial loading of data into RLS. The scope of the audit covered RLS operations during the period of July 1999 to March 2001. Audit emphasis was on OIG-defined vital control points for RLS security over and access to the RLS estimations database, the RLS closing database, the RLS national database, and the initial loading of data into the RLS national database.

Generally, to accomplish our audit objectives we reviewed and analyzed: (1) applicable security directives, procedures, and reports; (2) various RLS procedures, including the *Claims Manual*, *RLS Users Manual*, *RLS Operations Manual*, and *RLS Access Control Procedures*; and (3) RLS system documentation. We also interviewed personnel from DRR and DIRM who are responsible for supporting and operating RLS.

In addition, to determine whether the security environment over RLS was adequate, we toured the locations where the estimations and national databases and closing equipment were housed. During our “walk-throughs,” we observed the physical controls in place to protect the databases from theft

and unauthorized use. We did not observe a bank closing during our audit, therefore, our review of physical security during an actual bank closing was limited to our review of available security reports and procedures.

Regarding controls over access to the various RLS databases, we evaluated the levels of access granted to DRR and DIRM personnel for each of the three RLS database environments. Specifically, we identified all DIRM and DRR personnel with access to RLS and compared their level of access to their current job duties to determine whether such access was necessary. For the three RLS environments, we also reviewed all security reports and event logs to evaluate whether DIRM and DRR were adequately monitoring them.

Regarding controls over the initial loading of data into RLS, we identified three critical points of data entry. These critical data entry points were (1) the ongoing process of converting claims information from the three legacy systems, (2) the loading of information during the actual institution closing, and (3) the input of discovered liabilities into the national database (most of these were in the form of claims from general creditors that were not identified at the time of closing). Because we did not observe an actual bank closing during our audit, our assessment of closing controls was limited to reviewing available written policies and procedures and access security reports.

To identify vulnerabilities that could hamper the accurate and complete loading of data into RLS, we interviewed DIRM and DRR personnel responsible for this function and reviewed the data conversion plans, and policies and procedures. We also conducted an assessment of supervisory controls by attempting to enter data into the system. We did not perform any independent testing of the initial loading of data into RLS or of data conversions.

In addition, in May 2000, the DIRM information security staff completed an Independent Security Review (ISR) of RLS. Our report addresses concerns not included in the ISR report. The ISR report contained 32 recommended corrective actions to improve RLS operations. As of January 25, 2001, the information security staff had not formally issued the report to DIRM and DRR. Consequently, DIRM and DRR had not formally addressed the 32 recommended corrective actions. In the OIG's March 19, 2001 report entitled *Audit of the FDIC's Information Technology Risk Management Program* (Audit Report No. 01-007), we determined that DIRM could enhance the program's effectiveness by developing a tracking process capable of efficiently resolving corrective actions for the ISRs. In its response to the OIG's March 2001 report, DIRM stated that it would identify corporate officials responsible for the corrective actions, establish target dates for completing the actions, and track resolution of the actions.

Our audit included DRR and DIRM operations in Dallas, Texas, and the Washington, D.C., area. We conducted our audit from October 2000 to March 2001 in accordance with generally accepted government auditing standards.

RESULTS OF AUDIT

Generally, the FDIC established a good security structure for RLS. Specifically, DRR and DIRM developed RLS with two layers of access security: (1) read only access for those who need the information but do not need to load or change data and (2) read/write access for those who do need to load and change data. Also, DRR conducted reviews of initial access requests and semiannual security reviews of the national system to limit access to sensitive data. We did not identify a single occurrence of DRR or DIRM inappropriately granting original access to RLS. However, we found that better security reviews and additional security-related procedures would enhance system security.

Good procedures were in place for transferring data from the former systems to RLS. Data encryption technology had been added to help ensure that information transmitted from the bank closings was secure. Additionally, an audit table had been established with version 3.0 of RLS to capture user data changes and thereby permit management to review user activity. However, we believe that the chances for inaccurate or incomplete data loads can be further reduced by improving reconciliation procedures, verifying record count totals transmitted from bank closings to the national database, strengthening the data certification process, and improving storage of archived RLS audit tables.

SECURITY PROCEDURES NEED TO BE ENHANCED

Some current and former FDIC employees had RLS access they did not need. Also, DRR information security personnel did not routinely or sufficiently review security reports to identify inappropriate access to the national, estimations, and closing databases. DRR management could improve access controls by removing employee access to RLS as soon as employees change job responsibilities or leave the Corporation and by better monitoring RLS security reports.

Excessive Access to RLS Data

Access to the national and estimations databases was excessive. Specifically:

- Five of the 51 FDIC employees (10 percent) with national database access at January 10, 2001 did not need that access. Access for the five individuals had not been rescinded when their duty assignments changed because supervisors did not notify system security personnel of the changes.
- Thirty-five percent of the financial institution number (FIN) data write permissions¹ granted to 19 claims agents were granted to individuals that did not need the write permissions. In all, these 19 employees held 659 permissions to write to institution records. We found, when comparing the claims assignment worksheet that indicates employees' responsibilities for

¹ A permission is an authorization for a user to perform an action within a computer. In this case, a data write permission permits the user to enter or modify data in the computer. Without the write permission, the user would only be able to read the data in the computer.

FINs to the granted permissions, that 50 percent of the assigned write permissions were not supported by the claims assignment worksheet. However, after interviewing all employees who had been granted write permissions, we found that the actual number of excessive permissions granted was 35 percent, because the claim assignment worksheet did not accurately reflect all work assignments conducted by the claims agent.

- Six of the 22 DIRM employees (27 percent) on the SQL data input access lists at the time of our review in January 2001 did not need access because bank closing responsibilities had been removed from their duties. The 22 individuals were approved to send data to the national database from a closing. The shift in responsibilities for the six happened approximately 2 months prior to our January 2001 review.
- Ten of 14 DIRM database administrators (DBA) (71 percent) inappropriately remained on the listing of approved administrators after their duties were changed. A DBA's access to data is broad in order to fulfill their responsibility for the operation, safeguarding, integrity, and maintenance of the RLS database. These individuals should have been removed promptly from the approved list of administrators when their duties changed. A large number of DBAs were originally assigned to work with RLS during system development and implementation. However, DIRM reduced the number of DBAs necessary to support RLS after the application was implemented in 1999.
- Twelve of the 46 employees (26 percent) with estimations database access did not need it. The 12 employees either were no longer employed by the FDIC or had changed assignments to positions that did not require estimations database access. One individual still had access almost 2 months after resigning from the Corporation.

OMB Circular A-130, Transmittal 4, states that agencies will protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information. FDIC Directive 1360.15, dated March 24, 2000, states that sensitive automated information systems and data shall be protected from unauthorized access, disclosure, and use. The directive further states that access to sensitive systems shall be permitted only for FDIC business purposes as approved by a supervisor and program manager or their designee and that such access shall be terminated when it is no longer required or when access privileges have not been used for a predetermined period of time. We believe that when access to sensitive data extends beyond the timeframes necessary to conduct job duties, the risk of inappropriate data disclosure, use, or alteration is unnecessarily increased.

We discussed our concerns with DRR and DIRM managers who agreed with our observations for each of the issues discussed above. According to the DRR Data Steward and DRR Information Security Specialist, access was not updated to reflect employee reassignments because responsible DRR managers did not always submit changes to security personnel. Similarly, DIRM managers did not always submit changes to security personnel. When we brought our concerns to DIRM management's attention, they requested the responsible managers to terminate the access for the 10 DBAs and the 6 former closing team members during February

2001. Further, DRR managers informed us that they reassigned write permissions for claims section employees in February 2001.

Recommendations

We recommend that the Directors, DRR and DIRM, each:

- (1) Ensure that access privileges are removed for the employees with unnecessary access.
- (2) Ensure that supervisors notify security personnel of employee resignations and reassignments in a timely fashion so that access for employees who have left or been reassigned can be immediately terminated.

Security Monitoring Needs to be Improved

Security reports for the national, estimations, and closing databases were not always printed, reviewed, and thoroughly researched for anomalies, such as employees who had been granted access but had not logged onto the system. We also found that report review duties had not been properly assigned. Specifically:

- Claims managers told us that almost 1½ years after the system was put into operation, they had not printed and reviewed the write permissions security report. Further, we found that the security report for analyzing write permissions was incomplete because it did not display all granted access. Specifically, the report displayed 90 FINs per person, but two employees each had authorized access to more than 125 FINs.
- DRR's data steward and security personnel did not take exception to RLS national database security reports showing that 8 of the 51 FDIC employees (16 percent) who had access to the RLS national database had never (for over 1½ years) accessed the database with their initial "default password."² The default passwords did not expire after 90 days of non-use as do regular passwords. Consequently, the 90-day password expiration security feature in RLS did not automatically recognize the non-use and terminate the default password. A thorough review of security reports by security personnel, however, would have shown that the passwords had not been used. Circular 1360.10, dated November 24, 1997, states that system administrators shall immediately suspend or disable access privileges associated with user IDs left inactive. The risk of inappropriate disclosure and alteration is increased if access is not reviewed routinely to detect any access abnormalities.
- SQL server event logs, logs that capture access activity such as successful and failed log-ons, were not reviewed by DIRM staff. The National Institute of Standards and Technology

² This is the initial password established for a user to log onto the system for the first time. Once the user logs on for the first time with the default password, it activates the password tables so that a password expiration date is calculated. For RLS, a password expires 90 days after it is initially entered into the system.

(NIST) publication 800-14 states that a review of system-generated logs can detect security problems, including attempts to exceed access authority or gain system access during unusual hours. FDIC Circular 1360.10, dated November 24, 1997, further requires that system logs be monitored for invalid log-in attempts that deviate from the normal or accepted range and that such attempts should be noted in an exception report that is checked daily. A new version of RLS released on December 15, 2000 contained an SQL upgrade. The SQL upgrade required reassignments of SA and DBA permissions and responsibilities including the responsibility for reviewing the logs. As a result of the SQL upgrade requirements, DIRM reassigned permissions to SAs and DBAs. However, DIRM did not assign responsibilities for monitoring the SQL event logs. The SAs had the permissions necessary to monitor the

logs but had not been assigned the task. We believe that either the DBAs or SAs should be assigned both the permissions and event log monitoring duties.

- DIRM closing personnel did not always forward bank closing security reports that identify individuals given access to RLS at the closing to the DRR Information Security Specialist. *RLS Operations Manual*, section 3.3.5, states that the initial and final security report should be sent to Washington DRR Security. The security specialist could not provide us with bank closing security reports for 5 of the 14 institutions (36 percent) closed since July 1999. Of the five closings, both the initial and final security reports were missing for four closings and the other closing was missing one of the security reports. Further, from our review of procedures, security reports, and other information provided by the DRR security specialist, we could not identify that formal report reviews were conducted. For example, we noted that the DIRM RLS system development project manager and other DIRM staff had been granted claims user IDs to access live bank closing data. However, the security specialist did not provide us with documentation showing that these occurrences were always discovered and questioned as a result of security report reviews.

We discussed these items with DIRM and DRR managers who agreed with our findings. Further, DRR claims managers notified us on February 8, 2001 that they were writing new procedures for monitoring the write permissions monthly.

Recommendations

We recommend that the Director, DRR:

- (3) Establish written procedures for security report reviews.
- (4) Request that the number of displayed FINs be expanded in the next RLS update.
- (5) Add DRR security personnel to the employee notification listing of bank closings to ensure that they are aware that bank closing security reports should be forwarded to them.

We recommend that the Director, DIRM:

- (6) Assign the duties and permissions necessary so that either the system administrators or database administrators have both the necessary permissions and job duty responsibilities of event log monitoring.
- (7) Remind DIRM personnel to send the closing security reports to DRR security personnel as required by the Operations Manual.

Security Over the Estimations Database Server and Back-up Tapes Can Be Improved

The estimations database server and back-up tapes were not physically secured. The server and back-up tapes were located in an open cubicle within a building that had no security guard. Theoretically, anyone gaining access to the building could gain access to the estimations server and back-up tapes. The server and tapes contain a substantial quantity of very sensitive information on banks that failed and prospective bank failures. The data includes information on depositors' names, addresses, social security numbers, bank account numbers, and bank balances for every failure/potential failure since implementation of RLS in July 1999.

On January 8, 2001, we brought this problem to Dallas DIRM management's attention. Management immediately took action to move the server and back-up tapes to a secured location. Accordingly, because we observed that adequate security measures had been taken, we are making no formal recommendation regarding this issue in this report.

Because of the quantity of information maintained on the database (in that it goes back to July 1999), we believe that security could be improved by archiving information (removing data from the production environment and storing it on separate CD or tape media) on institutions for which data access is no longer required. Archiving the information would ensure that employees do not have access to more information than they need to do their jobs.

Recommendation

We recommend that the Directors, DIRM and DRR:

- (8) Work together to develop procedures for archiving information not being used routinely.

THE CHANCES FOR INACCURATE OR INCOMPLETE DATA LOADS CAN BE REDUCED

The potential for loading incorrect information into RLS was heightened for several reasons: claims agents did not always reconcile data entered into RLS to the final DOF pro forma liability amounts, DIRM personnel did not validate the electronically transmitted data sent from the bank closing to FDIC headquarters, DRR personnel did not completely verify the accuracy of data

converted from legacy systems to RLS, and DRR supervisory reviews were not conducted on data entered into the system.

Reconciliation Procedures Need to be Improved

Not all of the RLS Data Import Balancing Reports reconciliations, which balance DOF proforma data to depositor data by claim type, included reconciliations to the final DOF pro forma liability amounts. We reviewed the balancing reports for 12 of the 14 institutions closed since the inception of RLS in 1999. We did not review the reconciliations for the two most recent bank failures. The 12 institutions had deposits at closing totaling over \$1.5 billion. Claims agents could not provide the reconciliations for one of the twelve institutions we reviewed. We found that 7 of the 12 RLS Data Import Balancing Report reconciliations contained a total of \$461,627 in unresolved differences that were not adequately explained and documented. We also noted that another \$629,045 in reconciling items had been identified by claims, but we could not locate where adjustments had been made to RLS. Additionally, only 2 of the 12 balancing reports were signed and dated by the preparer and none indicated that any type of supervisory review was conducted. Further, the format for the reconciliations was not consistent from closing to closing.

According to the 1994 *Claims Manual*, which had not been updated to include RLS procedures, DRR claims personnel are responsible for accounting for the deposit and general creditor liabilities of a failed bank. The manual further explains that this responsibility begins with a reconciliation of claims records to the liability totals proven by the DOF pro forma team. However, because the manual did not include the specific reconciliation procedures to be used in the RLS environment, employees may not have known the specific steps they were to perform relative to reconciliations. Additionally, a standard reconciliation format would ease the preparation. Claims amounts need to be reconciled because incorrect claim amounts can result in incorrect payouts.

DRR management personnel agreed and stated that improvement in this area was a goal for 2001. DRR managers have held some preliminary discussions to outline revisions to claims policies and procedures.

Recommendations

We recommend that the Director, DRR:

- (9) Research the unresolved differences and, when warranted, make balancing adjustments. Document the reasons for not making adjustments.
- (10) Ensure that effective written reconciliation procedures are established for staff assigned claims duties. These procedures should include a standard format, require signatures of preparer and reviewer, require identification and documentation of the reconciling items, and provide instructions for making adjustments when necessary.

Verifying Record Count Totals Will Help Ensure Complete Data Transfers From Bank Closings to the RLS National Database

DIRM closing team personnel did not forward record count totals of claims files sent to DIRM headquarters personnel for loading into the SQL server national database. Closing team personnel sent e-mails to the DIRM project manager advising that the files had been sent, but the e-mails did not include record counts. At various stages of the closing process and while loading files onto the national database, such as after data compression, encryption, and decryption are completed, file size and record count are to be verified. However, the record counts were not communicated to and between the two transit points (institution and DIRM headquarters). The *RLS Operations Manual* contains no requirement to verify record counts between the two transit points. Record count verification is a quick way to ensure that data is not lost during the transmission process. We believe that the *RLS Operations Manual* should be updated to include this procedure.

Our position is further supported by the U.S. General Accounting Office (GAO). In its Federal Information Systems Control Audit Manual (FISCAM), GAO indicates that an entity may have a data control group that is responsible for reconciling control counts and control totals for data submitted by users with similar counts and totals generated during processing.

DIRM management personnel told us that they will incorporate the requirement to send record counts from closings to the national database in the next closing training session and will incorporate the requirement in the next update to the *RLS Operations Manual*.

Recommendation

We recommend that the Director, DIRM:

- (11) Update the *RLS Operations Manual* to include procedures for verifying record count totals for data transmitted from bank closings to DIRM personnel responsible for loading the information into the national database and implement the requirements as soon as possible.

The Data Certification Process Needs to Be Strengthened

Although DRR personnel researched data anomalies such as blank fields or the incorrect number of digits in a data field prior to converting three legacy systems' (CTS, AGS/APS, and UDRS) data to RLS, the data certification process did not include a comparison of the data to be converted to source documentation. Consequently, data integrity was reduced. We noted that DRR's Internal Review group conducted a data integrity review of CTS and RLS in March 2000 and identified error rates of over 30 percent in the CTS critical fields of claimant name and address. We believe that such inaccurate data could lead to erroneous disbursements. At the time of our review, DRR had not prepared a formal response to the DRR Internal Review outlining any planned corrective actions. DRR management explained to us that constrained resources precluded source document verifications on data converted from legacy systems. We

believe, based on the extent of errors found by DRR's Internal Review group, that a process to ensure accurate data is warranted.

Recommendation

We recommend that the Director, DRR:

- (12) Develop a data integrity review plan for RLS that includes a comparison of legacy system data to source documentation prior to conversion and a review of data already converted to RLS.

Procedures for Storage of Archived RLS Audit Tables Need to be Improved

Although supervisory personnel reviewed hardcopy documentation prior to data entry, they did not review for accuracy the data entered to RLS. In fact, the system does not have an automated supervisory review requirement for data entered into RLS. However, the DIRM RLS Project Manager informed us that audit tables had been established within the RLS version 3.0 release to capture data entered into RLS. From these audit tables, ad hoc reports could be run to capture all data entry activity in case supervisory review was needed or activity needed to be traced.

When we requested the record retention procedures for the audit tables, we were informed that they were incomplete. The existing procedures called for archival of the tables every 90 days followed by the purging of the data from the audit tables, but the procedures did not disclose where the archived records were to be stored. Additionally, the procedures did not identify that the DBA's ability to process the archival had been fragmented with the SQL upgrade discussed earlier in this report.

We found that at the date of inquiry on February 27, 2001, three archivals had been performed. The last archival was completed in mid-October 2000. The October 2000 archival was being retained in a contractor DBA's office and the other two were in the Project Manager's office. Storing the archived information in individuals' offices reduces the likelihood that requested ad hoc reports of user data entry activity can be provided (because of the potential for loss, media damage, data manipulation, etc.). Therefore, we believe that the archived information should be stored in a more secure location. In addition, contingency planning circulars require that information also be stored off-site to ensure the ability to continue operations in the event that the information at the primary location is destroyed or otherwise becomes unusable.

The DIRM Project Manager and DRR security officer stated that they would coordinate an improvement to the record retention procedures for audit table archiving.

Recommendation

We recommend that the Directors, DIRM and DRR:

- (13) Develop detailed archival and storage procedures that include the roles and responsibilities for DBAs and SAs and provide for a secure storage location, preferably off-site.

CORPORATION COMMENTS AND OIG EVALUATION

On May 30, 2001, we received written responses to our draft report from the Director of DRR and Director of DIRM (Chief Information Officer). DRR's response is presented in Appendix I of this report. DIRM's response is presented in Appendix II of this report. DRR and DIRM management agreed to enhance security reviews and develop additional security-related procedures. Further, DRR and DIRM management agreed to improve reconciliation procedures, verify record count totals transmitted from bank closings, strengthen the data certification process, and improve the storage of archived RLS audit tables. DRR reported that its corrective actions had been completed. DIRM reported that all corrective actions would be completed by August 31, 2001. The Directors' responses are not summarized here because the actions planned or completed are identical to those recommended.

The Corporation's response to the draft report provided the elements necessary for a management decision on each of the report's recommendations. Therefore, no further response to this report is necessary. Appendix III presents management's proposed actions on our recommendations and shows that there are management decisions for all recommendations.

CORPORATION COMMENTS



Federal Deposit Insurance Corporation
1910 Pacific Avenue, 2nd Floor, Dallas, TX-75201

Division of Resolutions and Receiverships

DATE: May 18, 2001

MEMORANDUM TO: Sharon M. Smith
Assistant Inspector General

THROUGH: Mitchell Glassman *Mitchell L. Glassman*
Director
Division of Resolutions and Receiverships

FROM: A. J. Felton, Deputy Director *A. J. Felton*
Dallas Field Operations Branch
Division of Resolutions and Receiverships

SUBJECT: Response to Draft OIG Audit Report # 2000-211
Receivership Liability System Security and Data Validation

Pursuant to above subject matter, this memorandum will serve to respond to the issues and recommendations outlined in the draft OIG Audit Report dated April 30, 2001.

IG Audit Recommendations:

That the Directors, DRR and DIRM, each:

- (1) Ensure that access privileges are removed for the employees with unnecessary access.**
- (2) Ensure that supervisors notify security personnel of employee resignations and reassignments in a timely fashion so that access for employees who have left or been reassigned can be immediately terminated.**

DFOB Response: DFOB agrees with the finding and recommendations.

(1) Corrective Action: On May 4, 2001 new internal department procedures entitled "Receivership Liability System (RLS) Security Controls" were developed and implemented. Included in these procedures is the responsibility for Claims Unit Chiefs to ensure that access privileges are removed for employees having unnecessary access.

(2) Corrective Action: On May 4, 2001 new internal department procedures entitled "Receivership Liability System (RLS) Security Controls" were developed and implemented. Included in these procedures is the responsibility for Claims Unit Chiefs to ensure that appropriate security personnel are notified of employee resignations and reassignments so that access for employees who have left or been reassigned can be immediately terminated.

IG Audit Recommendations:

That the Director, DRR:

- (3) Establish written procedures for security report reviews.**
- (4) Request that the number of displayed FINs be expanded in the next RLS update.**
- (5) Add DRR security personnel to the employee notification listing of bank closings to ensure that they are aware that bank closing security reports should be forwarded to them.**

DFOB Response: DFOB agrees with the finding and recommendations.

(3) Corrective Action: On May 4, 2001 new internal procedures entitled “Receivership Liability System (RLS) Security Controls” were developed and implemented. Included in these procedures is the responsibility for review of security reports.

(4) Corrective Action: As of April 11, 2001, DRR had requested that the number of displayed FINs be expanded in the next RLS update. Washington DRR and DIRM have already included this request on the enhancements for a future RLS release.

(5) Corrective Action: Washington DRR Claims staff will provide Washington DIRM Security personnel with a copy of the organizational chart for closings to ensure they are aware that bank closing security reports should be forwarded to them. The Senior Receivership Management Specialist, Washington DRR, has agreed to assume responsibility for this action as of May 11, 2001.

IG Audit Recommendations:

That the Director, DIRM:

- (6) Assign the duties and permissions necessary so that either the system administrators or database administrators have both the necessary permissions and job duty responsibilities of event log monitoring.**
- (7) Remind DIRM personnel to send the closing security reports to DRR security personnel as required by the Operations Manual.**

DFOB Response:

- (6) Corrective Action:** Please refer to DIRM response
- (7) Corrective Action:** Please refer to DIRM response

IG Audit Recommendation:

That the Directors, DIRM and DRR:

(8) Work together to develop procedures for archiving information not being used routinely.

DFOB Response: DFOB agrees with the finding and recommendations.

(8) Corrective Action: On May 4, 2001, new internal department procedures entitled, "Receivership Liability System (RLS) Security Controls" were developed and implemented. Included in these procedures is the requirement that DRR DFOB Claims will review the Estimations Database every 6 months to determine if any of the information housed in the system is still relevant. If the information is no longer relevant, DRR Claims will delete the information.

IG Audit Recommendations:

That the Director, DRR:

(9) Research the unresolved differences and, when warranted, make balancing adjustments or document the reasons for not making adjustments.

(10) Ensure that effective written reconciliation procedures are established for staff assigned claims duties. These procedures should include a standard format, require signatures of the preparer and reviewer, require identification and documentation of the reconciling items, and provide instructions for making adjustments when necessary.

DFOB Response: DFOB agrees with the finding and recommendations.

(9) Corrective Action: On May 16, 2001 a review of the unresolved differences noted in this audit was completed by Claims Unit personnel. Based upon this review, Management has made the decision that balancing adjustments are not warranted. This decision is documented and is available for review.

(10) Corrective Action: DRR Claims Management has established written reconciliation procedures for staff assigned claims duties at closings, as documented by Internal Procedure entitled, "Reconciliation of Liability Accounts at Closing". Closing Reconciliation Training is being conducted for Claims staff beginning May 22, 2001 and subsequent sessions as necessary.

IG Audit Recommendation:

That the Director, DIRM:

(11) Update the RLS Operations Manual to include procedures for verifying record count totals for data transmitted from bank closings to DIRM personnel responsible for loading the information into the national database and implement the requirements as soon as possible.

DFOB Response: DFOB agrees with the finding and recommendations.

(11) Corrective Action: Please refer to DIRM response

IG Audit Recommendation:

That the Director, DRR:

(12) Develop a data integrity review plan for RLS that includes a comparison of legacy system data to source documentation prior to conversion and a review of data already converted to RLS.

DFOB Response: DFOB agrees with the finding and recommendations.

(12) Corrective Action: Internal Claim Procedures entitled, “Data Quality Program- Procedures”, were approved and implemented March 14, 2001 addressing data quality within RLS. In accordance with the internal procedures, semi-annual reviews are conducted and critical data elements contained within RLS are reviewed against source documents. Errors as identified are corrected and a summary report is prepared which provides an overview of the review, summarizing the error rates and details any corrective action plan that may be required as a result of the review.

IG Audit Recommendation:

That the Directors, DIRM and DRR:

(13) Develop detailed archival and storage procedures that include the roles and responsibilities for DBAs and SAs and provide for a secure storage location, preferably offsite.

DFOB Response: DFOB agrees with the finding and recommendations.

(13) Corrective Action: DRR has requested that DIRM archive information from the audit tables and maintain this archived data in a secure location for a period of 7 years. DIRM has accepted responsibility for developing formal procedures addressing this matter.

CORPORATION COMMENTS




Federal Deposit Insurance Corporation
3501 Fairfax Dr., Arlington, VA 22226

Office of the Chief Information Officer

May 30, 2001

TO: Sharon M. Smith
Assistant Inspector General

FROM: Donald C. Demitros, Chief Information Officer 

SUBJECT: DIRM Management Response to the Draft OIG Report Entitled, "Receivership Liability System Security and Data Validation" (Audit Number 2000-211)

The Division of Information Resources Management (DIRM) has reviewed the subject draft audit report and generally agrees with the findings and recommendations. Responses have been provided to the recommendations directed specifically to DIRM (recommendations 6, 7, and 11) as well as those which were directed to both DIRM and DRR (recommendations 1, 2, 8, and 13).

Management Decision:

We recommend that the Directors, DRR and DIRM, each:

- (1) Ensure that access privileges are removed for the employees with unnecessary access.
- (2) Ensure that supervisors notify security personnel of employee resignations and reassignments in a timely fashion so that access for employees who have left or been reassigned can be immediately terminated.

DIRM Response:

In response to the first two recommendations, DIRM database administrators will remove employees' access as requested by DRR Information Security Officers (ISO's) through FACES. The procedures to request removal are outlined in the DRR RLS Security Procedures. The DIRM Data Management Section (DMS) will conduct periodic reviews of database administrators access to ensure the timely removal of DIRM employees. Likewise DMS will ensure these removals upon staff reassignment or resignation. The designated DIRM closing team members have access to the shared area where closing data is downloaded for import into the national system. The Dallas DIRM Deputy Regional Manager maintains the current listing of DIRM closing team members and provides the DIRM DRR Software Management Section (SMS) with any required team member changes. All authorizations for access to that shared area are authorized and controlled by DIRM DRR SMS.

We recommend that the Director, DIRM:

- (6) Assign the duties and permissions necessary so that either the system administrators or database administrators have both the necessary permissions and job duty responsibilities of event log monitoring.

DIRM Response:

DIRM is currently in the process of implementing a new intrusion detection capability that will provide DIRM Information Security Section (ISS) the ability to centrally monitor both NT and SQL event logs. The product, Intruder Alert (ITA), will monitor 100 Windows NT based servers. Twenty percent of these servers are the SQL servers. With full implementation August 31, 2001, ITA will monitor Windows NT System, Security, and Application event logs. ITA will also be capable of monitoring SQL Server error logs. This new technology coupled with centralized security monitoring will address this recommendation. In the interim, NT event logs and SQL error logs are being copied to a shared drive by the DIRM LAN Management Section. DIRM ISS will provide these logs to the DRR ISO for review until ITA is fully operational.

- (7) Remind DIRM personnel to send the closing security reports to DRR security personnel as required by the Operations Manual.

DIRM Response:

The DIRM Bank Closing Team was reminded to send the closing security reports to DRR security personnel during a refresher RLS DIRM Operations Training class that was given January 29 – 31, 2001. Additionally the current Operations Manual, dated December 12, 2000, includes a “RLS Application Security Closing Worksheet” that contains a reminder to send the closing security reports to DRR security personnel.

We recommend that the Directors, DIRM and DRR:

- (8) Work together to develop procedures for archiving information not being used routinely.

DIRM Response:

The data on the Estimations server was deleted on January 23, 2001 when the Estimations server was upgraded to SQL Server v7.0/RLS v5.0. DRR determined that the data on the server at the time was no longer relevant. Based on DIRM discussions with DRR, DRR will review the Estimations Database every six months to determine if any of the information housed in the system is still relevant. If the information is no longer relevant, DRR will delete the data. DRR has determined that there is no business or legal requirement to archive the estimations database.

We recommend that the Director, DIRM:

- (11) Update the *RLS Operations Manual* to include procedures for verifying record count totals for data transmitted from bank closings to DIRM personnel responsible for loading the information into the national database and implement the requirements as soon as possible.

DIRM Response:

DIRM will draft procedures to verify record count totals by July 31, 2001 and finalize the procedures by August 31, 2001. The procedures will be included in the *RLS Operations Manual*. The next release of RLS, scheduled for implementation in mid-December, will provide an automated means to verify the record count totals.

We recommend that the Directors, DIRM and DRR:

- (13) Develop detailed archival and storage procedures that include the roles and responsibilities for data base administrators and systems administrators and provide for a secure storage location, preferably off-site.

DIRM Response:

DIRM will draft the requested archival and storage procedures by July 31, 2001 and finalize the procedures by August 31, 2001.

Please address any questions to DIRM's Audit Liaison, Rack Campbell, on (703) 516-1422.

cc: Vijay Deshpande
Ken Jones
Janet Roberson
Wayne Gooding

MANAGEMENT RESPONSES TO RECOMMENDATIONS

The Inspector General Act of 1978, as amended, requires the OIG to report the status of management decisions on its recommendations in its semiannual reports to the Congress. To consider FDIC's responses as management decisions in accordance with the act and related guidance, several conditions are necessary. First, the response must describe for each recommendation

- the specific corrective actions already taken, if applicable;
- corrective actions to be taken together with the expected completion dates for their implementation; and
- documentation that will confirm completion of corrective actions.

If any recommendation identifies specific monetary benefits, FDIC management must state the amount agreed or disagreed with and the reasons for any disagreement. In the case of questioned costs, the amount FDIC plans to disallow must be included in management's response.

If management does not agree that a recommendation should be implemented, it must describe why the recommendation is not considered valid. Second, the OIG must determine that management's descriptions of (1) the course of action already taken or proposed and (2) the documentation confirming completion of corrective actions are responsive to its recommendations.

This table presents the management responses that have been made on recommendations in our report and the status of management decisions. The information for management decisions is based on management's written response to our report [optional: and subsequent discussions with management representatives].

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Documentation That Will Confirm Final Action	Monetary Benefits	Management Decision: Yes or No
1	Appropriate personnel from DIRM and DRR will monitor access privileges.	Completed	Copy of RLS Security Controls procedures.	N/A	Yes
2	Supervisory personnel from DIRM and DRR will notify security personnel of staffing changes to terminate access.	Completed	Copy of RLS Security Controls procedures.	N/A	Yes
3	On May 4, 2001, procedures were issued that assigned responsibility for the review of security reports.	Completed	Copy of RLS Security Controls procedures.	N/A	Yes
4	An enhancement to the software was requested April 11, 2001.	Completed	Copy of enhancement list.	N/A	Yes

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Documentation That Will Confirm Final Action	Monetary Benefits	Management Decision: Yes or No
5	DRR security personnel will be provided the closing organization chart as of May 11, 2001.	Completed	Organization charts forwarded to security.	N/A	Yes
6	Interim practices will be followed by new intrusion detection capability, which should be implemented by August 31, 2001.	August 31, 2001	Evidence of log reviews or new capability being implemented.	N/A	Yes
7	Employees were reminded to forward the security reports in a January 29 – 31, 2001 training session.	Completed	Copy of training materials.	N/A	Yes
8	DRR will review the data on the estimation server every 6 months and delete unneeded information as outlined in procedures issued May 4, 2001.	Completed	Copy of RLS Security Control procedures	N/A	Yes
9	On May 16, 2001 a review of the unresolved differences was completed.	Completed	Documentation related to the review.	N/A	Yes
10	A procedure entitled <i>Reconciliation of Liability Accounts at Closing</i> was issued and training sessions will be held starting May 22, 2001.	Completed	<i>Reconciliation of Liability Accounts at Closing</i> procedures.	N/A	Yes
11	Procedures for verifying the record count totals will be drafted by July 31, 2001 and added to the <i>RLS Operations Manual</i> by August 31, 2001.	August 31, 2001	Updated procedures	N/A	Yes
12	New <i>Data Quality Program Procedures</i> were implemented March 4, 2001 requiring semi-annual review of critical RLS data elements.	Completed	<i>Data Quality Program Procedures</i>	N/A	Yes
13	DRR requested DIRM to develop formal archiving procedures. The procedures will be drafted by July 31, 2001 and finalized by August 31, 2001.	August 31, 2001	Updated procedures	N/A	Yes